SPECIFICATION AMENDMENTS

Please replace the title with this new title:

Stealthy Secret Key Encoding and Decoding

Before the heading "Technical Field", please insert the following section at the beginning of the specification:

RELATED APPLICATIONS

This is a continuation of U.S. Patent Application Serial No. 10/641,684, filed August 14, 2003.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

Please replace paragraph 155 with the following paragraph:

[0155] In at least one example implementation that includes image watermarking on printed media, the exemplary secret key distribution secretly encodes the secret key into and/or around the physical manifestation of the marked goods. For example, the exemplary secret key distribution system may clandestinely encode a version of the secret key around the watermarked image in the form of a border that consists of "light" and "dark" pixels. In this implementation, a "dark" (resp. "light") pixel may correspond to a 1 (resp.0), hence conveys 1 bit of information. It is also possible to use more than 2 levels for such a PAM (pulse amplitude modulation) system. For instance, in another implementation of our system, we may use 2^r different gray levels for each pixel of the border, in which case each pixel conveys r bits of information. Naturally, this constitutes a tradeoff between the bit-error rate that is introduced by scanning and the total number of bits conveyed. In our system, we experimentally found that the 2-level amplitude modulation (i.e., using "light" and "dark" pixels to convey 1 bit of information) yields satisfactory results.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

Please replace paragraph 157 with the following paragraph:

[0157] In order to achieve this purpose, the exemplary secret key distribution uses pseudo-randomly generated error-correction code for encoding purposes. A master key is used to generate such an error-correction code. The exemplary secret key distribution uses a secret error-correction code instead of conventional encryption schemes in order to further correct possible errors that may happen during the printing and scanning process. The exemplary secret key distribution employs an algebraic linear block codes for the generation of the secret error-correction code. However, other implementations may employ other types of error-correction codes that are well-known in the coding theory literature (e.g., non-algebraic codes, iteratively decodable product codes, etc.)

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

Please replace paragraphs 161 and 162 with the following paragraphs:

[0161] At 810, the encoder pseudo-randomly generates p different generator matrices $\mathbf{G}_i$ in Galois-Field2 (GF2), $1 \leq i \leq p$. Note that each $\mathbf{G}_i$ is of size $(n/p) \times (m/p)$ and it should be full-rank. Without loss of generality, it is assumed that p divides both n and m.

[0162] One way to achieve full-rank generator matrix construction in GF2 is to generate each $\mathbf{G}_i$ in its systematic form. That is $G_i = \left[I_{(n/p)\times(n/p)} \mid R_{(n/p)\times(m/p-n/p)} \right]$, where $I_{(n/p)\times(n/p)}$ is the identity matrix of size $(n/p) \times (n/p)$ and $R_{(n/p)\times(m/p-n/p)}$ is a pseudo-random binary matrix of size $(n/p) \times$ (m/p - n/p). In other words, each entry of $\mathbf{R}$ is 0 or 1 with probability ½. This construction guarantees that $\mathbf{G}_i$ is full-rank (rank (n/p)) and furthermore each full-rank matrix can be reduced to such systematic form.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

Please replace paragraph 166 with the following paragraph:

[0166] At 818, it produces **y** on the periphery of the watermarked signal. In the case of a printed image, it prints **y** surrounding the watermarked image in the form a border that consists of "light" and "dark" pixels, where "light" (resp. "dark") corresponds to a 1 (resp. 0). In the case of audio, it may encode **y** in the "noise" outside the range of human hearing in the frequency domain or before/after the beginning/end of the clip in the time domain.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com
lee&hayes

Please replace paragraph 168 with the following paragraph:

[0168] Let $\mathbf{z} \in \{0,1\}^m$ be the input of the decoder. The input $\mathbf{z}$ could be obtained, for example, by scanning a printed image, such as what is illustrated in Fig. 2. Furthermore, it is assumed that the secret *master* key K and the corresponding system parameters m, n, p are known at the decoder. The goal here is to find out the secret key that determines the embedded watermark.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com
lee&hayes

Please replace paragraph 173 with the following paragraph:

[0173] Fig. 10A shows an example of a marked image without the boundary information carrying the secret key. Fig. 10B shows an example of the same marked image, but it now includes the boundary information carrying the watermark-specific secret key.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com
lee&hayes